Таблица 1

Методические подходы к подготовки будущих специалистов по защите корпоративных систем к agile-управлению проектами

<table>
<tr><td rowspan="2">Системный подход (структура модели; компонентный состав, элементы, внутрисистемные связи и т. д.)</td><td>Компетентностный подход</td><td>Проектный подход</td></tr>
<tr><td colspan="2">Специфика формируемого у будущих специалистов по защите информации качества — готовности к agile-управлению проектами</td></tr>
</table>

Список литературы

1. *Сабельников С. А.*, *Астахова Л. В.* Методика реализации педагогических условий развития проектно-управленческих компетенций будущих специалистов по защите информации // Вестн. УрФО. Безопасность в информационной сфере. 2016. № 3. С. 47–55.

2. *Сабельников С. А.*, *Астахова Л. В.* Модель развития компетенций в области управления проектами по защите информации в вузе // Вестн. Челяб. гос. пед. ун-та. 2016. № 4. С. 76–84.

3. *Бадейко В. И.* Выявление состава компетенций выпускников вуза как необходимый этап проектирования ГОС ВПО нового поколения : метод. пособие. М. : Исслед. центр проблем качества подготовки специалистов, 2006. 72 с.

4. *Астахова Л. В.* Управленческая компетенция специалиста по защите информации : монография. Челябинск : Изд. центр ЮУрГУ, 2014. С. 78–80.

5. *Махотин Д. А.* Проектный подход к технологии обучения в системе высшего профессионального образования // Качество. Инновации. Образование. 2005. № 1. С. 11–21.

УДК 342.922/951

В. В. Суровцев, А. Е. Поляков
Научный руководитель: ст. преп. В. М. Жернова
Южно-Уральский государственный университет, Челябинск

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

Аннотация. В статье рассматривается одни из наиболее острых вопросов в сфере информационной безопасности в сети Интернет — информационная безопасность личности и способы ее достижения. Отмечается, что в социальных сетях и мессенджерах, а также в открытых точках доступа к сети Интернет нарушается конфиденциальность личности. В статье приведен обзор нормативных правовых документов.

Ключевые слова: сеть Интернет; конфиденциальность; безопасность личных данных; защита информации.

Информационная безопасность личности в сети Интернет означает состояние и условие нахождения личности в информационном пространстве сети Интернет, использование различных сайтов и мессенджеров, при которох реализуются ее права и свободы.

Социальные сети позволяют субъектам свободно общаться и обмениваться информацией. Существует множество примеров, когда информация в социальных сетях становится доступной третьим лицам в позитивных целях, таких как помощь спецслужбам, поиск пропавших лиц с помощью интернет-ресурсов для организации работы волонтеров и прочее.

К сожалению, ввиду того, что пользователи сами оставляют много персональной информации, например для заполнения аккаунтов социальных сетей и профилей в интернет-магазинах, применение данных, полученных в ходе анализа такой информации может повлечь за собой негативные последствия.

Говоря о сборе, обработке и передачи третьим лицам личной информации о пользователе социальной сети, можно привести пример известной сети «ВКонтакте». В статье В. Велюги года проходит исследование трафика, отправляемого приложением «ВКонтакте» с мобильного устройства [1]. В результате чего обнаруживается, что данная социальная сеть, помимо своих метрик и телеметрий, отправляет такие данные о пользователе и его устройстве, как:

– текущее местоположение мобильного устройства;
– характеристики ближайших точек доступа в сеть Интернет;
– все действия, осуществляемые на смартфоне;
– считывается вся информация о самом устройстве, в том числе и данные о сим-карте.

Конечно, в пользовательском соглашении (правилах пользования) прописано, что «ВКонтакте» передают информацию, но без указания конкретных третьих лиц: «Администрация сайта вправе использовать предоставленную Пользователем информацию, в том числе персональные данные, а также передавать ее третьим лицам, в целях обеспечения соблюдения требований действующего законодательства Российской Федерации, защиты прав и интересов пользователей, Администрации сайта, третьих лиц (в том числе в целях выявления, проверки/расследования и/или пресечения противоправных действий)» [2].

Также при более полном анализе трафика и исходного кода приложения «ВК» можно обнаружить, что данные сохраняются на сервер и передаются третьим лицам. Главными представителями являются MyTracker и LibVerify, а также MailRuGroup и сервис Vigo.

В наше время существуют сообщества, воздействующие на сознание человека через различные социальные сети. И если раньше людей зазывали в секты на улицах, то сейчас гораздо эффективнее делать это через Интернет, ведь вся информация о людях изложена на их же страницах. Дети и подростки постоянно находятся онлайн и общаются в социальных сетях, выкладывают множество информации о себе, тем самым делая свои персональные данные общедоступными. Очень легко увидеть то, чем занимается человек, о чем он думает, есть ли у него проблемы и какие они. Вербовщик или сектант подходит к этому делу очень тщательно, ищет более внушаемого и открытого человека.

Например, очень нашумевшая игра «Синий кит», распространяемая через социальные сети, например, «ВКонтакте». Чаще всего в игру заманиваются дети и подростки, так как их сознание наиболее уязвимо.

Подобных и других сект очень много, как и организаторов и участников таких групп, которые воздействуют на сознание человека в негативных целях. Поэтому нужно быть осторожным. Любая личная информация, выкладываемая в социальных сетях, представляет большую опасность для владельца таких данных. Вопросам безопасности детей и подростков в сети Интернет посвящают свои исследования многие ученые [3].

Нелегальную информацию и товары легче всего найти в так называемом Darknet (Темный интернет). Darknet — это часть сети Интернет, в которой можно найти все то, что нельзя найти в легальном сегменте. В Темном интернете производится торговля наркотиками, оружием, людьми и т. д. Государству сложно контролировать Темный интернет, так как домены сайтов могут меняться каждый день. Вход в Темный интернет производится благодаря браузеру Tor, браузер использует систему VPN. В Темном интернете оплачивают все с помощью криптовалют, так как они дают анонимность покупателю и продавцу. В темной Сети есть множество социальных сетей, но с определенным контингентом, к примеру социальная сеть по обсуждению наркотиков и их приготовления и многие другие примеры.

Федеральный закон № 276 «О внесении изменений в закон „Об информации, информационных технологиях и о защите информации“» не запрещает пользоваться VPN-сервисами и анонимайзерами. Речь идет лишь о том, что с их помощью теперь нельзя будет наведываться на запрещенные сайты [4]. Таким образом, в России с помощью закона намерены бороться с распространением экстремистских материалов и другой запрещенной информации.

Но и в обычных социальных сетях производится продажа незаконной продукции. К примеру, в социальной сети «ВКонтакте» тоже продают наркотики, оружие и многое другое, только это происходит не так открыто, как в Darknet. Как это происходит в «ВКонтакте»: создаются страницы-«однодневки» с использованием не отслеживаемого мобильного телефона и на определенных

форумах выкладывается информация об этой страницей. На самой странице уточняется, что и где можно забрать/купить.

Подводя итог, можно сказать: социальные сети — это способ всегда быть на связи с друзьями и семьей, но также их можно использовать со злыми намерениями. Поэтому нужно быть более внимательным и ответственным по отношению к себе, осознавать необходимость распространения персональных данных.

Стоит запомнить некоторые правила, позволяющие сделать жизнь как можно безопаснее:

1. Пароль. Придумывайте как можно более сложный и длинный пароль. Проявите фантазию в создании своего пароля: не стоит использовать в качестве пароля дату рождения, клички животных и др. Используйте название стихотворения, дату какого-нибудь события в истории и многое другое. Добавляйте в свой пароль символы, иностранные буквы, цифры. Для каждой социальной сети придумывайте свой пароль — так безопасность ваша и ваших страниц будет увеличена.

2. Меньше личной информации. В своем профиле пишите как можно меньше о себе, ваших поездках, номерах телефонах и др. В такой социальной сети, как Instagram, пользователи рассказывают о своем распорядке дня, своем местоположении, личной информации о себе и так далее.

3. Фотография. Перед тем как выложить фотографию, внимательно посмотрите на каждую деталь: на свой внешний вид, на окружающую местность, людей, находящихся рядом с вами, и многое другое.

4. Конфиденциальность. Установите параметры конфиденциальности. Незнакомые вам люди не должны видеть важные сведения о вас, которые могут быть расположены на странице.

5. Безопасные браузеры. Используйте только надежные и проверенные браузеры, не забывайте про брандмауэр и антивирусную программу. Также не переходите на социальную сеть по случайным ссылкам из Интернета.

6. Никогда не переходите на незнакомые ссылки, которые присылают неизвестные вам люди. Не открывайте подозрительные сообщения. Мошенники с легкостью подлавливают таким образом людей и информацию о них, вплоть до взлома вашей страницы.

7. Проверка приложений. Перед тем как установить то или иное приложение, тщательно узнайте о нем и его безопасности, чтобы не попасться на уловку.

8. Общаясь с друзьями в сетях, будьте внимательны. Их страницы могут быть взломаны. На любое подозрительное сообщение от друга отреагируйте немедленно. Позвоните другу и убедитесь, он ли это вам отправил.

9. Знакомства. С осторожностью относитесь к выбору друзей. Если к вам добавляется незнакомый человек или присылает вам сообщение, тщательно подумайте, стоит ли отвечать ему. Быть может, это серьезно навредит вам.

10. Не используйте файлообменные сайты для получения пиратских программ, ведь вместо них может быть вирус.

11. Wi-Fi. Будьте осторожны при использовании Wi-Fi. Обычно почти каждый человек, увидев то, что нашлась бесплатная точка доступа, сразу подключаются к ней. А это может подвергнуть вас опасности. Если у вас есть возможность пользоваться сетью Virtual Private Network, которая позволяет вам работать в защищенной частной сети при общедоступном подключении, то обязательно воспользуйтесь.

С другой стороны, использование средств-анонимайзеров для соблюдения анонимности в сети Интернет и VPN для получения нелегального контента запрещена на государственном уровне — за этим следят ФСБ и Роскомнадзор.

Со стороны ФСТЭК следует отметить, что необходимо соблюдать простые требования безопасности для защиты данных от вредоносного программного обеспечения. Так, существует некоторое количество вирусов, которые перенаправляют информацию из мессенджеров с компьютеров и смартфонов. В случае, если на компьютере обрабатывается информация, содержащая персональные данные третьих лиц, необходимо соблюдать требования ФСТЭК по защите такой информации [5].

Всегда будьте начеку и соблюдайте правила, тогда возникновение неблагоприятных последствий от распространения персональных данных будет сведено к минимуму.

Список литературы

1. «ВКонтакте» уличили в сборе данных о пользователях [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2017/08/01/727286-v-kontakte-dannih-polzovatelyah (дата обращения: 28.10.2017).

2. Правила пользования сайтом «ВКонтакте» [Электронный ресурс]. URL: vk.com/terms (дата обращения: 28.10.2017).

3. *Рубцова О. В.* Безопасная среда для детей в информационном обществе // Вестн. УрФО. 2016. № 1(19). С. 39–44.

4. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» : Федеральный закон № 276-ФЗ от 29.07.2017 // Рос. газета. 2017. № 172.

5. Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty.